INFORMACIÓN SOBRE EL PRODUCTO DE AKAMAI

Información sobre el producto Brand Protector

Detecte y bloquee sitios de phishing, tiendas falsas y suplantaciones de marcas: evite las consecuencias perjudiciales para sus clientes y reduzca el riesgo de ataques de fraude y uso indebido a gran escala.

Una marca distintiva genera un valor cuantificable tanto dentro como fuera de la organización. Al proteger los elementos que se asocian con su marca podrá mantener y fidelizar a sus clientes, reducir las pérdidas y las reseñas negativas, y aumentar la productividad. Desde el punto de vista de la seguridad, el control de la suplantación de una marca neutraliza una intrusión de raíz, impidiendo la recopilación de credenciales y la usurpación de cuentas.

Sin embargo, no todos los ataques se inician en la puerta de entrada de una organización. En la web, los atacantes suplantan su marca para robar los datos confidenciales, las credenciales y la información de los pagos directos de sus clientes. La suplantación de marca y el phishing presentan un desafío cada vez mayor, ya que, en sus campañas de corta duración, las ubicaciones van variando y solo son visibles de forma intermitente, lo que obliga a dedicar una gran cantidad de recursos para la detección y la mitigación.

Akamai Brand Protector usa una de las mayores bases de datos de inteligencia contra amenazas, que combina fuentes de datos propias y de terceros, para acelerar las detecciones y mejorar la precisión. Las capacidades integradas de mitigación hacen de Brand Protector una herramienta eficaz y esencial para la detección temprana de ataques de fraude y abuso.

Akamai Brand Protector detecta y mitiga los ataques dirigidos, lo que incluye el phishing, la suplantación de identidad y el abuso de marca en sitios web, redes sociales y tiendas de aplicaciones. Y, lo que es más importante, Brand Protector le ayuda a preservar la confianza de sus clientes.

Cada semana se crean más de 50 000 nuevos sitios web de phishing. Brand Protector inspecciona billones de actividades digitales al día, procedentes de fuentes internas y externas, para detectar de manera rápida y eficaz los abusos relativos a la marca y los elementos de marca de su empresa, a menudo antes de que se inicie una campaña de ataque.

Para lograr todo esto, Brand Protector aborda el problema de la suplantación fraudulenta con nuestro enfoque de cuatro pasos: inteligencia, detección, visibilidad y mitigación.

Ventajas para su empresa

Detección fiable de ataques
Nuestra exclusiva red global y las fuentes adicionales nos ofrecen una ventaja única para detectar las suplantaciones de marcas.

Velocidad y precisión
Nuestra rápida detección algorítmica es capaz de generar alertas antes de que se lancen las campañas de ataque y minimiza los falsos positivos.

Información práctica
Se ofrecen datos completos como información útil con una puntuación de riesgo que resume la gravedad y el alcance de un ataque de un solo vistazo.

Visibilidad por cliente
Acceda a una recopilación de datos específicos de su marca, sus productos y elementos asociados en sitios web, redes sociales y tiendas de aplicaciones.

Facilidad de uso
Obtenga información en tiempo real e inicie la corrección de este vector de ataque cada vez mayor en unos minutos.

Neutralización y mitigación
Mantenga su productividad con el servicio de neutralización integrado de Brand Protector o interrumpa el tráfico con una alerta de navegación.

Inteligencia

Los desafíos que plantea detectar el phishing y los ataques de suplantación de marca comienzan en la fase de inteligencia y recopilación de datos.

Como plataforma en el Edge y en la nube más grande del mundo, Akamai cuenta con una visión exclusiva del tráfico web global, ya que analizamos más de 788 TB de datos al día. La extraordinaria inteligencia de Brand Protector se ha mejorado con fuentes de datos de terceros para garantizar una visibilidad integral de las acciones de los atacantes. Además, puede añadir su propia URL y dominios para que el sistema de detección en la nube de Brand Protector los analice.

Detección

La potencia y velocidad de detección de Brand Protector provienen de una combinación de fuentes de información y algoritmos de análisis propios de Akamai, diseñados para aumentar la fiabilidad de la detección y reducir los falsos positivos.

Los ataques a la marca automatizan sitios web maliciosos de corta duración. La mayoría de las tecnologías no son lo suficientemente rápidas a la hora de detectar y mitigar estos recursos de ataque antes de que afecten negativamente a los clientes. El enfoque de Akamai es diferente porque, en lugar de recurrir a listas actualizadas o fuentes diferidas, analizamos el tráfico en tiempo real para detectar los abusos de marca. Gracias a Brand Protector, su equipo de seguridad puede detectar sitios de phishing cuando se produce la primera solicitud HTTP/HTTPS, normalmente antes de que la campaña llegue a sus clientes.

Visibilidad

La labor de ingeniería y el diseño centrados en el cliente proporcionan a su equipo una gran cantidad de información sobre la seguridad en un panel de control centralizado.

Tras recibirse la información, las señales de datos se procesan a través de una serie de detectores heurísticos y de inteligencia artificial. Si bien se recopila una cantidad abrumadora de datos y pruebas, la interfaz de usuario simplificada de Akamai proporciona una comprensión rápida de las amenazas de suplantación actuales que sufren sus clientes.

El tráfico, las detecciones y los datos de amenazas específicos del cliente se traducen en información procesable en el portal de clientes de Akamai. Los resultados se clasifican según una puntuación de amenaza. Los usuarios pueden hacer clic en una alerta para ver los datos de amenazas analizados, lo que incluye la puntuación de confianza, la clasificación de gravedad, el número de usuarios afectados y una cronología de los eventos de ataque.

Cada amenaza detectada está respaldada por pruebas. Puede ver códigos, capturas de pantalla, indicadores de la detección y datos del dominio en una única pantalla de detección.

Mitigación

Los servicios de neutralización integrados cierran el ciclo en la lucha contra el fraude de marca.

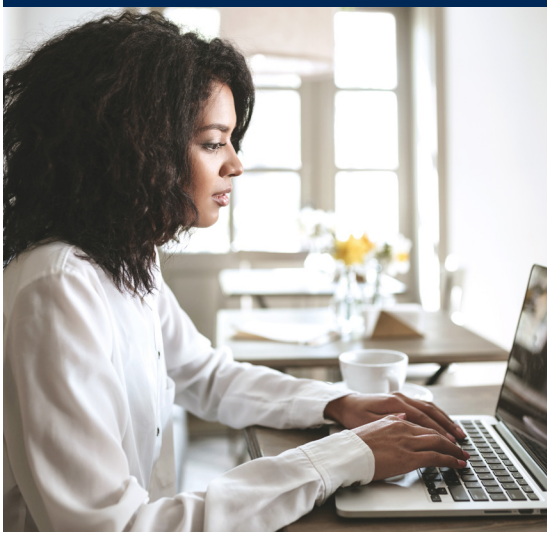
Brand Protector permite a su equipo emitir una solicitud de bloqueo del sitio abusivo directamente desde la pantalla de detección. A las solicitudes de neutralización (enviadas a un partner externo de Akamai) de Brand Protector se adjuntan automáticamente las pruebas de la detección de la amenaza y otros datos relevantes que mejoran su comprensión. Puede realizar un seguimiento y ver el estado de la mitigación en el portal.

Diseñado para su marca

Protección por zonas
Esta solución de nuestra cartera de productos de protección en el Edge amplía la visión de su equipo para garantizar la seguridad en las primeras fases de la intrusión. Busca de forma proactiva permutaciones de los dominios de su marca que podrían utilizarse para lanzar ataques de phishing a los clientes.

Supervisión de redes sociales
Con el aumento de la suplantación de marcas en las redes sociales, nuestra nueva función mejorada de supervisión de redes sociales detecta y neutraliza el fraude online para proteger a su marca y a sus clientes en varias plataformas.

Detección de aplicaciones no autorizadas
La supervisión de tiendas de aplicaciones es una nueva función que analiza repositorios de aplicaciones oficiales y extraoficiales para detectar aplicaciones engañosas que hacen un uso indebido de la identidad de la marca, lo que supone una defensa completa en todo el entorno digital.



©2024 Akamai Technologies | Asistencia | | Publicado en noviembre de 2024